APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/851,625	05/08/2001	Rajasekhar Sistla	P10212	3678

50890   7590   12/09/2008
CAVEN & AGHEVLI
c/o INTELLEVATE, LLC
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER
TRUONG, LAN DAI T

ART UNIT	PAPER NUMBER
2452	

MAIL DATE	DELIVERY MODE
12/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>03</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>29 October 2008</u>.

2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-21</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-21</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/29/2008 has been entered.

2. This action is response to communications: application, filed on 05/08/2001; amendment filed on 10/29/2008. Claims 1-21 are pending; claims 1, 5-6, 11 and 17 are amended.

3. The applicant's arguments filed on 10/29/2008 have fully considered but they are moot in view with new ground for rejections.

Response to Arguments

4. In response to applicant's amendments to independent claim 17, the previous rejection under 35 USC § 101 for claim 17 is withdrawn. However, the previous rejections under 35 USC § 101 for claims 18-21 are retained.

5. In regard to the newly amended limitations to claims 1, 6, 12 and 17, the examiner has provided further citations from the reference to show the teachings of the newly amended features (see rejection below for details).

Claim rejections-35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-21 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Regarding claim 1:

The claim(s) contains subject matter (i.e. irrespective of the recipient's email address) which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Nowhere in the specification discloses the use of restricting the recipient's ability to modify contents of the electronic mail based on… irrespective of the recipient's email address. Without disclosures the use of restricting the recipient's ability to modify contents of the electronic mail based on irrespective of the recipient's email address from the specification; how would one of ordinary skill in the art determine claim limitation of "restricting the recipient's ability to modify contents of the electronic mail based on… irrespective of the recipient's email address." Appropriate corrections are required.

Regarding claims 2-21:

Those claims are rejected under rationales of claim 1.

Claim rejections-35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill

in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the
invention was made.

Claims 1-11 and 17-21 are rejected under 35 U.S.C 103(a) as being un-patentable

over Gupta et al. (U.S. 2002/0099777) in view of Chaudhari et al. (U.S. 7,039,951) and

further in view of Spraggs (U.S. 6,941,454).

Regarding claim 1:

Gupta discloses the invention substantially as claimed, including a method, which can be

implemented in a computer hardware or software code for preserving confidentiality of an

electronic mail from a sender to a recipient, the method comprising:

authenticating identity information of the recipient: (In Gupta's mailing system, a receiver

is requested to provide user IDs and Passwords for authentication process:[0130]; [0131]).

restricting the recipient's ability to modify contents of electronic mail based on

irrespective of the recipient's email address: (in Gupta's collaborative email message, sender is

capable of selecting recipients whom be restricted from modifying the received collaborative

email messages by adding those recipients into 'bcc' list. It would have been obvious in the art to

understand that email recipient's address should be included in 'bcc' list: [0062]-[0063]; [0065],

lines 10-15; [0081], lines 16-22).

 However, Gupta does not explicitly disclose establishing confidentiality levels by the

sender.

In analogous art, Chaudhari discloses method for establishing confidential levels for

email recipients so that the mailing system can be able to calculate and determine if the

recipients are authorized to read the emails those are stored in a secured database based on

assigned confidential levels, see (Chaudhari, column 3, lines 23-29; column 5, lines 1-67;

column 8, lines 1-40; column 9, lines 32-34).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine Chaudhari's ideas of providing users confidentiality-based

authentication into Gupta's system in order to increase secure levels for communication system,

see (Chaudhari, column 1, lines 7-14).

However, Gupta-Chaudhari does not explicitly disclose steps of encrypting the electronic

mail, at the recipient, with the authenticated identity information if the recipient attempts to store

the electronic mail to a local storage.

In analogous art, Spraggs discloses a server is capable to re-encrypt the decrypted data

those are received from a sending client with the server key and store the re-encrypted data into a

secure database, see (Spraggs, column 3, lines 45-51).

decrypting the electronic mail, at the recipient if the recipient attempts to retrieve the

electronic mail from the local storage: (Spraggs further discloses the server decrypts the stored

re-encrypted data when it attempts to retrieve the data from the secure database responsive to

client requests, see (Spraggs, column 3, lines 45-67).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine Spraggs's ideas of providing a server capability of re-encrypting

data prior storing them into a secure database into Gupta-Chaudhari's system in order to provide

higher secure level communication system, see (Spraggs, column 1, lines 44-47).

Regarding claim 2:

In addition to rejection in claim 1, Gupta-Chaudhari-Spraggs further discloses wherein the identity information is a system password: (In Gupta's mailing system, a receiver is requested to provide user IDs and Passwords for authentication process: [0130]; [0131]).

Regarding claim 3:

In addition to rejection in claim 1, Gupta- Chaudhari- Spraggs further prompting a user of the recipient to supply the identity information: (a receiver is requested to provide user IDs and Passwords for authentication process: Gupta, [0130]; [0131]).

decrypting the electronic mail with the identity information supplied by the user: (In Spraggs's system, the receiving client can decrypt data via using it's private key: column 3, lines 65-67).

Regarding claim 4:

In addition to rejection in claim 1, Gupta-Chaudhari-Spraggs further discloses asserting a control signal to disable options that are originally supported by the recipient if the confidentiality level satisfies a predefined confidentiality threshold: (in Gupta's mailing system, created collaborative email can be set up with numbers of options (e.g. email encryption, preventing recipient from modifying email, storing message, setting prior status and/or confidential): [0065]; [0060]-[0061]; figure 3; figure 4).

Regarding claim 5:

In addition to rejection in claim 4, Gupta-Chaudhari-Spraggs further discloses the control signal is a control signal: (Gupta: [0065]; [0060]-[0061]; figure 3; figure 4).

Regarding claim 17:

Gupta discloses the invention substantially as claimed, including a storage device, which can be implemented in a computer hardware or software code for preserving confidentiality of an electronic mail from a sender to a recipient, the method comprising:

authenticating identity information of the recipient: (In Gupta's mailing system, a receiver is requested to provide user IDs and Passwords for authentication process:[0130]; [0131]).

restricting the recipient's ability to modify contents of electronic mail based on irrespective of the recipient's email address: (in Gupta's collaborative email message, sender is capable of selecting recipients whom be restricted from modifying the received collaborative email messages by adding those recipients into 'bcc' list. It would have been obvious in the art to understand that email recipient's address should be included in 'bcc' list: [0062]-[0063]; [0065], lines 10-15; [0081], lines 16-22).

However, Gupta does not explicitly disclose establishing confidentiality levels by the sender.

In analogous art, Chaudhari discloses method for establishing confidential levels for email recipients so that the mailing system can be able to calculate and determine if the recipients are authorized to read the emails those are stored in a secured database based on assigned confidential levels, see (Chaudhari, column 3, lines 23-29; column 5, lines 1-67; column 8, lines 1-40; column 9, lines 32-34).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chaudhari's ideas of providing users confidentiality-based authentication into Gupta's system in order to increase secure levels for communication system, see (Chaudhari, column 1, lines 7-14).

However, Gupta-Chaudhari does not explicitly disclose steps of encrypting the electronic mail with the authenticated identity information if the recipient attempts to store the electronic mail to a local storage.

In analogous art, Spraggs discloses a server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database, see (Spraggs, column 3, lines 45-51).

decrypting the electronic mail if the recipient attempts to retrieve the electronic mail from the local storage: (Spraggs further discloses the server decrypts the stored re-encrypted data when it attempts to retrieve the data from the secure database responsive to client requests, see (Spraggs, column 3, lines 45-67).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Spraggs's ideas of providing a server capability of re-encrypting data prior storing them into a secure database into Gupta-Chaudhari's system in order to provide higher secure level communication system, see (Spraggs, column 1, lines 44-47).

Regarding claim 18:

This claim is rejected under rationale of claim 2.

Regarding claim 19:

This claim is rejected under rationale of claim 3.

Regarding claim 20:

This claim is rejected under rationale of claim 4.

Regarding claim 21:

This claim is rejected under rationale of claim 5.

Regarding claim 6:

Gupta discloses the invention substantially as claimed, including an electronic mail confidentiality preserver of a recipient email client, which can be implemented in a computer hardware or software code, comprising:

an input-processing engine to limit abilities of a user of the recipient email client to modify contents of an electronic mail received by the recipient email client based upon irrespective of the recipient's address: (in Gupta's collaborative email message, sender is capable of selecting recipients whom be restricted from modifying the received collaborative email messages by adding those recipients into 'bcc' list. It would have been obvious in the art to understand that email recipient's address should be included in 'bcc' list: [0062]-[0063]; [0065], lines 10-15; [0081], lines 16-22).

an encryption/ decryption engine, coupled to the input-processing engine, to encrypt the electronic mail with authentication identity information: (in Gupta's mailing system, created collaborative email can be set up with numbers of options (e.g. email encryption and/ or preventing recipient from modifying email). It would obvious to one of ordinary skill in the art to recognize that Gupta's system should include encryption/decryption engine: [0065]; [0060]).

However, Gupta does not explicitly disclose confidentiality level.

In analogous art, Chaudhari discloses method for establishing confidential levels for email recipients so that the mailing system can be able to calculate and determine if the recipients are authorized to read the emails those are stored in a secured database based on assigned confidential levels, see (Chaudhari, column 3, lines 23-29; column 5, lines 1-67; column 8, lines 1-40; column 9, lines 32-34).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chaudhari's ideas of providing users confidentiality-based authentications into Gupta's system in order to increase secure levels for communication system, see (Chaudhari, column 1, lines 7-14).

However, Gupta-Chaudhari does not explicitly disclose encrypting email if the recipient attempts to store the electronic mail to a local storage.

In analogous art, Spraggs discloses a server is capable to re-encrypt the decrypted data those are received from a sending client with the server key and store the re-encrypted data into a secure database, see (Spraggs, column 3, lines 45-51).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Spraggs's ideas of providing a server capability of re-encrypting data prior storing them into a secure database into Gupta-Chaudhari's system in order to provide higher secure level communication system, see (Spraggs, column 1, lines 44-47).

Regarding claim 7:

This claim is rejected under rationale of claim 4.

Regarding claim 8:

This claim is rejected under rationale of claim 5.

Regarding claim 9:

In addition to rejection in claim 6, Gupta- Chaudhari- Spraggs further discloses the input processing engine further asserts a second control signal to invoke the encryption/decryption engine in response to the user's access: (Spraggs: column 3, lines 65-67; column 4, lines 1-2).

Regarding claim 10:

In addition to rejection in claim 6, Gupta-Chaudhari-Spraggs further discloses prompting the user for identity information: (Spraggs: figure 7, items 710, 712).

decrypting the electronic email with the identity information: (Spraggs: figure 7, items 710, 712).

encrypts the electronic mail with the identity information to store the electronic mail: (Spraggs: figure 7, item 708; column 3, lines 45-51).

decrypts the electronic mail to retrieve the electronic mail: (the receiving client can decrypt data via using it's private key: Spraggs: column 3, lines 65-67).

__Regarding claim 11:__

Gupta discloses the invention substantially as claimed, including an electronic mail client, comprising:

a user interface: (Gupta: figure 2; figure 3).

a communication engine: (Gupta, figure 3, item 142).

a local storage: (Gupta discloses client device also has capability of storing information locally (e.g. user preferences, identifiers, email messages…etc): [0044]; figure 10, item 286).

an electronic mail confidential preserver, coupled to the user interface, coupled to the communication engine and coupled to the local storage: (in Gupta's system, user can interact with mailing client device through a interface/ display window, wherein user can select numbers of mailing options (e.g. storing message, setting prior status and/or confidential) : figure 3; figure 4; [0061]).

an input-processing engine to limit abilities of a user of the recipient email client to modify contents of an electronic mail received by the recipient email client based upon irrespective of the recipient's email address: (in Gupta's collaborative email message, sender is capable of selecting recipients whom be restricted from modifying the received collaborative email messages by adding those recipients into 'bcc' list. It would have been obvious in the art to understand that email recipient's address should be included in 'bcc' list: [0062]-[0063]; [0065], lines 10-15; [0081], lines 16-22).

an encryption/ decryption engine, coupled to the input-processing engine, to encrypt the electronic mail with authentication identity information: (in Gupta's mailing system, created collaborative email can be set up with numbers of options (e.g. email encryption and/ or preventing recipient from modifying email). It would obvious to one of ordinary skill in the art to recognize that Gupta's system should include encryption/decryption engine: [0065]; [0060]).

However, Gupta does not explicitly disclose confidentiality level.

In analogous art, Chaudhari discloses method for establishing confidential levels for email recipients so that the mailing system can be able to calculate and determine if the recipients are authorized to read the emails those are stored in a secured database based on assigned confidential levels, see (Chaudhari, column 3, lines 23-29; column 5, lines 1-67; column 8, lines 1-40; column 9, lines 32-34).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chaudhari's ideas of providing users confidentiality-based authentications into Gupta's system in order to increase secure levels for communication system, see (Chaudhari, column 1, lines 7-14).

However, Gupta-Chaudhari does not explicitly disclose encrypting email if the recipient

attempts to store the electronic mail to a local storage.

In analogous art, Spraggs discloses a server is capable to re-encrypt the decrypted data

those are received from a sending client with the server key and store the re-encrypted data into a

secure database, see (Spraggs, column 3, lines 45-51).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine Spraggs's ideas of providing a server capability of re-encrypting

data prior storing them into a secure database into Gupta- Chaudhari's system in order to provide

higher secure level communication system, see (Spraggs, column 1, lines 44-47).

Claims 12-16 are rejected under 35 U.S.C 103(a) as being un-patentable over Gupta-

Chaudhari-Spraggs in view of Bennett (U.S. 6,760,704).

Regarding claim 12:

In addition to rejection in claim 11, Gupta- Chaudhari-Spraggs further discloses a set of

options to manipulate the electronic mail for the user to select: (Gupta discloses interface

provides various user-selectable options e.g. viewing, creating, and manipulating email: ([0097];

[0085]).

However, Gupta-Chaudhari- Spraggs does not explicitly disclose set of confidential

levels for the user to select.

In analogous art, Bennett discloses user can prompt sensitive condition for message, see

(Bennett, column 10, lines 6-11).

Thus, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Bennett's ideas of using prompting information for selecting confidentiality levels into Gupta-Chaudhari-Spraggs's system in order to increase conveniences for system users and to save resources and development time by implying Bennett's ideas into Gupta-Chaudhari-Spraggs's system.

Regarding claim 13:

In addition to rejection in claim 12, Gupta-Chaudhari-Spraggs-Bennett further discloses asserting a control signal to disable options that are originally supported by the recipient if the confidentiality level satisfies a predefined confidentiality threshold: (Gupta, [0065]; [0060]-[0061]; figure 3; figure 4).

Regarding claim 14:

In addition to rejection in claim 13, Gupta-Chaudhari-Spraggs-Bennett further discloses the control signal is a control signal: (Gupta, [0065]; [0060]-[0061]; figure 3; figure 4).

Regarding claim 15:

In addition to rejection in claim 12, Gupta-Chaudhari-Spraggs-Bennett further discloses the input processing engine further asserts a second control signal to invoke the encryption/decryption engine in response to the user's access: (Spraggs: column 3, lines 65-67; column 4, lines 1-2).

Regarding claim 16:

In addition to rejection in claim 12, Gupta-Chaudhari-Spraggs-Bennett further discloses prompting the user for identity information: (Spraggs: figure 7, items 710, 712).

decrypting the electronic email with the identity information: (Spraggs: figure 7, items 710, 712).

encrypts the electronic mail with the identity information to store the electronic mail: (Spraggs: figure 7, item 708; column 3, lines 45-51).

decrypts the electronic mail to retrieve the electronic mail: (the receiving client can decrypt data via using it's private key: Spraggs: column 3, lines 65-67).

Conclusions

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LAN-DAI Thi TRUONG whose telephone number is (571)272-7959. The examiner can normally be reached on Monday- Friday from 8:30am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A. Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

12/05/2008.

/Kenny S Lin/

Primary Examiner, Art Unit 2452